ISSN. 1363-6650

SEPTEMBER 1998
Issue 21

International Journal of FORENSIC COMPUTING™

Contents

International Journal of Forensic Computing

Third Floor, Colonnade House,
High Street, Worthing,
West Sussex, UK
BN11 1NZ

Tel: +44 (0) 1903 209226
Fax: +44 (0) 1903 233545
e-mail:ijfc@pavilion.co.uk
http://www.forensic-computing.com

Comment

All too often computer criminals are seen as a breed apart from the "normal" class of offender.

The media, public and even the police and court systems are sometimes guilty of glamorising these culprits simply because a sophisticated computer has been used as a crime tool instead of a crowbar or a getaway car.

It's easy to fall into the trap of thinking that just because a man wears a shirt and tie and knows his way around often complex software that he is somehow different from any other perpetrator.

A certain mystique hangs over those who use technology to commit crime - a bubble that needs to be burst.

In reality a crime is still a crime, no matter how it is carried out, and the techniques used in the subsequent investigaton are very similar.

There is no miracle button that when pressed can automatically find and retrieve evidence from a suspect's computer. As the science of forensic computing develops, better and more efficient hardware and software is produced to help the investigator.

But no matter how sophisticated the forensic tools, the success or failure of any case boils down to plain old detective work on the part of the analyst.

As with all criminal enquiries it is vital to understand the suspect and his or her motives in order to find out more about how the offence was committed and what evidence there is.

That is why the article on page 19 of this issue is so important. It takes a look at how to expedite an investigation by taking the time to find out a little more about the suspect.

Even just a few basic background details can reap huge rewards and save hours of fruitless time looking for the wrong files in the wrong place.

No amount of clever investigation software or computing power can help if the investigator doesn't know what he's after in the first place.

Many computer criminals worldwide still think that they are smart enough to outwit police and law enforcement agencies unused to computer investigations.

Once this might have been the case, but the gap is shrinking fast and we are beginning to see a new breed of investigators who have the experience and the capability to do the job properly.

Internet child pornography is a recurrent theme in Journal articles. It seems in just about every issue we report on an arrest or conviction of an online paedophile somewhere in the world.

But the recent investigation and raids of Net abusers across the globe is somewhat different. It marks a watershed both in the attitudes of police forces and the ability to co-operate with each other effectively.

Make no mistake, this was a huge operation, both in terms of the paedophile ring itself and the detective teams set up in a host of countries to investigate it.

The success of the police and customs officers cannot be measured in the number of arrests or convictions or even the amount of child pornography recovered.

For the real rewards are reaped by the innocent children who have been subjected to abuse and may now be spared further suffering, or just as importantly, the youngsters who are now saved from suffering a similar fate.

News

US e-signature laws

A survey commissioned by the US Internet Law & Policy Forum shows 47 of the nation's states are either considering or have already enacted some variation of the electronic authentication law.

Only Arkansas, South Carolina, and South Dakota have resisted the trend, according to a study conducted by the Washington, DC law firm Perkins Coie LLP. The forum will use the results in developing model legislation.

At stake, according to lawmakers, are billions of dollars in savings for government and business entities that often see agreements stalled while awaiting physical signatures to make them valid.

Not wanting to be left out is Oklahoma, which joined the fold when Gov. Frank Keating signed Oklahoma's Electronic Records and Signature Act (HB 3287) earlier this year.

"This will be a real economic development tool for Oklahoma that will increase our credibility as a state on the cutting edge of technology," Keating said.

Still, despite overall enthusiasm for the concept, there has been little uniformity in approaches to electronic authorisation laws.

Many states are opting for a minimalist approach - providing only that an electronic signature shall not be rejected on legal grounds solely because of its electronic form - while others are drafting hybrid laws that address the actual form of electronic and digital signatures.

Under hybrid legislation, lawmakers establish evidentiary presumptions in favour of the user of an electronic signature based on security and trustworthiness standards. No one seems to agree which form is best.

State-to-state differences have spilled over into the national and international arenas. The National Conference of Commissioners on Uniform State Laws is drafting a recommendation that will pursue a version that leans most toward a minimalist approach, while the United Nations Commission on International Trade Law has recommended the hybrid approach.

The lack of uniformity and cross-border recognition standards among the states means that no one knows whether an electronic signature will be considered valid outside of the jurisdiction in which it was affixed. If recognised, there is still the question as to which state's law will apply.

Canadian security agencies fear hackers

Canadian security agencies fear the country's sensitive data banks are vulnerable to hackers, says the Canadian Security Intelligence System.

According to documents obtained by a newspaper, using the Access to Information Act, CSIS has conducted a series of briefings for several federal departments aimed at sensitising them to a growing cyber break-in threat.

The Canadian Department of Defence is also reportedly working with the United States military to devise measures to keep intruders out of sensitive military computer sites.

"We take the matter quite seriously and we do consider it something that necessitates us taking a good, hard look at it," said CSIS spokesman Marcia Wetherup.

The newspaper article says that since last October, CSIS has held briefing sessions for six agencies, including National Defence, Immigration, the Supreme Court of Canada, and an association of federal employees with sensitive security clearances.

Concern is growing in intelligence circles that future conflicts or terrorist attacks could target electronic networks due to growing dependence of governments on computer-based communication and information technologies.

The CSIS, responsible for advising the government of potential threats, sees the Internet and other electronic tools as new means for extremists to sabotage vital institutions or steal valuable information.

The agency warns that individuals or groups could do extensive damage to power grids, communication and transportation systems as well as stock markets and financial institutions.

"Such attacks could have wide-ranging social, economic and political ramifications," CSIS maintains, and adds that the Canadian situation is characterised by a lack of awareness of computer security dangers, as well as the absence of "a formal structure to deal with the issue."

According to documents, the CSIS briefings also discuss recent attempts to breach American military systems and the methods and tools used by cybercriminals.

Authorities identify three types of hackers: neophyte, skilled and elite. "The first two categories are the ones that are caught by enforcement agencies," the briefing material states.

"The elite hacker seems to be able to operate within networks and systems without being detected."

The briefings describe many hackers as young computer fanatics who enjoy the excitement of entering forbidden territory - a thrill that has landed several cyber-joyriders in jail.

For CSIS, the hacker threat hit close to home several months ago when an unknown intruder entered the service's Website and altered the logo. The Royal Canadian Mounted Police Website has reportedly been similarly breached.

However, both agencies insist no intruders have yet compromised their sensitive information holdings, which are kept separate from their Internet sites.

The CSIS presentation features a list of 28 Canadian federal departments and agencies that are alleged to have been hacked. But the agency stresses the list, found on the Internet, was not compiled by the service and was included merely to warn departments to the perceived threat.

For security reasons, CSIS won't reveal how many federal agencies have actually been breached but the RCMP says the growing popularity of the Internet has created more opportunities for infiltration as hackers prowl the global network seeking the electronic equivalent of unlocked doors.

"I think it is becoming a bigger problem every day," said RCMP Inspector Fred Lyle, the officer in charge of the force's high-tech crime forensic section, who added: "We're getting calls periodically from departments saying that peo-

ple are attempting to hack into their systems.

"I don't think, to my knowledge, that we've had anybody break into any of the sensitive systems."

However, Lyle told the newspaper, if there was a serious breach, a department might be caught unaware. "Unless they have an active program watching for that, they don't know that they're being attacked."

The Canadian and US militaries are reportedly teaming up to defend their computer networks from cyber attacks. The alliance could eventually be expanded to protect civilian networks such as banking and power systems.

CSIS lists some technologies used by cyber-intruders to break into secure systems:

Password-sniffers: Gather passwords and other data going over a network.

Password-crackers: Match log-in attempts against a password dictionary.

Worms: Virus-like programs that can be tailored to seek entry into specific systems.

Secret writing tools: Used to hide coded material in sound, text or other types of files.

Further information: http://www.rcmp-grc.gc.ca/html/cpu-cri.htm

http://www.csis-scrs.gc.ca/index.html

New Thai Internet group forms

Members of the Thai chapter of the Internet Society, suspended from the main society since January, have formed a new society, the Internet Society in Thailand.

The Thai chapter (ISOC-TH) was suspended from the Internet Society (ISOC) in January by action of the Board of Trustees following a controversy over the chapter's part in a proposed Thai Internet law.

ISOC vice president of chapters Vint Cerf said the suspension was "because its president was taking public positions considered incompatible with ISOC principles."

The controversy began when the Legal Committee of the ISOC-TH became involved in the drafting of the Internet Promotion Act. The proposed law received widespread attention and criticism.

The proposed Article 11 prohibited dissemination on the Internet of information including anything against the peacefulness of society, immoral, inappropriate material concerning the King and the Royal Family, pornography, material discrediting the nation or the Government and and other issues.

Additional controversy was drawn by the proposed Article 16, which set conditions for becoming an Internet provider or content provider.

These included the conditions that such people must be well-behaved, have a respected profession, not be declared a delinquent person under the law, and never have been sentenced to jail for any serious matter.

Following the press coverage of the new law and subsequent revelation that the ISOC-TH was involved in its drafting, the ISOC requested its chapter play not part in the formation of the new law.

It also addressed its members in Thailand, asking them to oppose the law. "We see a danger that the law could lead to a government censorship committee that would attempt to exercise broad and heavy-handed control over the Internet," it said in a message to members.

"The least amount of law affecting the Internet is the best amount."

The investigation into the ISOC-TH charter continues and is expected to be completed soon, said Cerf, "In the course of the review, it was concluded that a review of the bylaws would also be appropriate.

This review should be completed by the end of August, at which time recommendations for change, if any seem appropriate, will be conveyed to the chapter."

In the meantime, Prof. Dr. Srisakdi Charmonman, widely regarded as the father of the Thai Internet and chair of the ISOC-TH, has formed the Internet Society, Thailand, a legally registered society in the country and independent of the ISOC-TH.

Its charter outlines objectives of the new society as promoting education, research and applications of Internet and related technologies; disseminating Internet knowledge to staff members and executives of government agencies, government enterprises and private organisations, as well as to students and instructors of academic institutions and members of other societies; and exchanging Internet knowledge and experience with other organisations and societies both in Thailand and abroad.

The group names the ISOC-TH suspension as one of two reasons for the formation of the new group. The second is the ISOC's membership fees, which are charged in US dollars and are currently 1,400 baht.

This fee is, "rather expensive in view of the present economic crisis in Thailand," explained the new group, which is charging members 100 baht per year.

The lower prices seem to be attracting users. The Internet Society in Thailand, currently has 20,000 members against just 300 members of the ISOC-TH, but the groups are not competitors. Almost all ISOC-TH members have joined the new group.

Digital copyright bill

Online copyrights could be protected in the US within months, after the US House of Representatives approved a compromise bill.

The proposed law is designed to keep artistic and creative works safe from pirating, while at the same time ensuring liability limitations on telephone companies and Internet service providers.

The act, HR 2281, the Copyright Treaties Implementation Act, would make the necessary amendments to US law to enable the Senate to ratify the World Intellectual Property Organisation's treaties negotiated last year in Geneva. Its Senate counterpart, S 1121, passed the Senate last May on a 99 to 0 vote.

The bill also would prohibit knowingly providing false copyright management information with intent to induce or conceal software piracy and other copyright infringement. This would protect ISPs from copyright infringement for unknowingly distributing unauthorised copyrighted material.

The compromise bill will now go to

a joint Senate-House conference committee and then to the President for his signature.

Despite the near unanimous passage in the Senate and the House, the bill, introduced by Rep. Howard Coble (R-NC) last July, took more than a year of compromise, wrangling and haggling between the competing interests of the creative content providers, including musicians, writers, software developers and entertainers, and the distribution providers, such as telephone companies and ISPs.

"Both sides need each other," Rep. Bob Goodlatte (R-Va.) said.

The compromise legislation, US Telephone Association President and Chief Executive Roy Neel said, would "benefit copyright owners by providing a method to protect intellectual property" online, and would give phone companies and ISPs "the assurance that they will not be subjected to costly lawsuits based on corrupt activity conducted by their customers."

Along with protecting ISPs, the legislation passed by the House also would allow for "fair use" of copyrighted materials by schools and libraries, and compromised on circumvention of encryption safeguards designed to protect digital creative works.

Under the compromise, anti-circumvention rule would be delayed for two years while the Commerce Department and the US Patent and Trademark Office study the problem.

But a group of nearly 50 security researchers and practitioners delivered a letter to Congressional leaders urging them to reconsider provisions of the copyright protection legislation, fearing that the same "technological protection measures" that could be used to protect digital works on the Internet also are used to protect users against computer viruses and perform security tests of commercial network installations.

The "experts" asserted that if the bill was passed, many vital forms of security testing might be rendered illegal.

The bill "fails to further recognise that encryption research is simply one aspect of security research, and that research is different from actual practice," Eugene Spafford, author of the letter and an information security expert, said. "While it may exempt encryption research, it still criminalizes other crucial techniques used in security research and practice."

Debit card fraud linked to Net

Fraudulent charges made against some bank account holders in the US may have had a link to the Internet.

Some account holders at the Transportation Federal Credit Union in Washington DC have lost as much as $5,000 through their Visa debit cards.

The credit union's president said that investigators are looking at the possibility that the debit card - also known as check cards - numbers were generated by software created by computer hackers, who posted the program to the Internet.

While most of the account numbers spat out by the software do not work, some of the numbers do, the credit union official said.

The credit union official would only say that fewer than half of the 2,600 accounts at the institution were affected by unauthorised charges. The official also said that the credit union is also establishing new security measures to prevent such an occurrence in the future.

Online chat confessor

The man who gained notoriety for confessing to an online chat group that he killed his daughter by torching their house will reportedly enter a guilty plea for the crime.

Larry Froistad, who has been in jail on charges related to the murder, has reportedly reached a plea agreement with Bowman County, North Carolina authorities in the three-year-old case.

Details of the plea agreement are not being made public at this time, but a person guilty of murder in North Carolina can face a sentence of up to life in prison, with no chance for parole.

Froistad allegedly posted several messages to an online support group for problem drinkers that he set fire to his house in 1995, while his five-year-old daughter Amanda slept in her bedroom.

Members of the online group turned in Froistad, even though they faced criticism over the revealing of details that were supposed to be kept only among members of the group.

Investigators also found pornography on a computer owned by Froistad, who is a computer programmer, press reports said. Evidence found in the computer also indicated that he molested his daughter, authorities said.

Froistad is also reportedly set to plead guilty to federal pornography charges following the discovery of the material, reports said.

Hacker had Navy Net address

An official with a British conservation group alleges that someone using a US Navy computer at the Pentagon tried to hack into the group's server.

In an e-mail to the media, the group claimed that an unknown user at the Pentagon tried and failed three times to breach a secure link on a Web server used by the Whale and Dolphin Conservation Society located in Bath, England.

The alleged attempts tripped an alarm in the system's security software. The WDCS webmaster then traced the hacking attempts to donhqns1.hq.navy.mil, a server address at the Pentagon, WDCS said.

WDCS said it quickly alerted the American embassy in London, but a Navy spokesperson in Washington said the service had not yet received a formal complaint.

"Until we receive the formal complaint and review what happened," the Navy spokesman said, "we can't proceed further.

"The claim that someone at the Navy was identified as the end user is false," he said. "The address is a Navy server, a machine with thousands of end users.

The US Navy has a strict policy against misuse of government material, including computer hardware and software. Any allegation that any Navy material was used to conduct any felony activity will be investigated."

The WDCS had previously spoken out on "quite a few issues that involve

the US Navy," said Frances Clarke, WDCS' campaign co-ordinator.

The Navy had requested a WDCS report on the export of former Soviet military dolphins several weeks before the alleged hacking attempts, Clarke said.

Clarke said the alleged hacker might have been a curious Navy researcher trying to "go too far."

The WDCS monitors its Web site to analyse visitor interest, including monitoring the frequency of hits and most-visited links. If visitors try to get to secure sites, the security system kicks in and tracks their activities, Clarke said.

In this instance, the hacker "identified the software we're using for the Web server," said Matt Penton, technical director of Merchant Technology Ltd. of Bath, England, the Internet service provider used by the conservation society.

WDCS does not plan to pursue the matter further. The group's goal is to "just publicise the fact that they tried to do that so it doesn't happen again," Clarke said. "We're lucky we had a security system in place," she said.

New e-mail bug found in Eudora

First, researchers discovered a security flaw in Microsoft's Outlook 98 and Outlook Express and Netscape's Communicator e-mail packages.

Now, a flaw appears to be affecting Windows versions of Qualcomm's Eudora 4.0, 4.01 and 4.1 e-mail programs.

Reports said the flaw could allow a computer hacker, more accurately known as a cracker, to put a virus on computers that run the Eudora program.

A manager at Qualcomm said that a cracker could send Eudora users an e-mail with an attachment that could potentially either erase or put a virus on a user's hard drive.

The damage would happen when the unsuspecting user clicked on a hostile link in the message - instead of linking to the page, the action would start the attached file, which would then wreak its havoc.

Qualcomm said it has not heard of anyone being affected by the flaw, and that a patch would be available on its Web site.

US SEC Internet Enforcement

The Securities and Exchange Commission in the US is fighting fraud by forming a new enforcement unit to combat the threat of cyber crime.

"While the Internet has many benefits, a small group of thieves is trying to hijack unsuspecting investors on the information superhighway," Richard H. Walker, director of the SEC's Enforcement Division, said.

According to Walker, the SEC already has brought more than 30 cases involving Internet related securities fraud to date, covering virtually every type of investment scam, including phoney offerings, market manipulations, affinity frauds that target a particular ethnic or religious group, and pyramid and ponzi schemes.

The new unit will be an expansion of the Commission's Enforcement Complaint Centre, the SEC's online communications centre on the World Wide Web, which currently receives more than 120 complaints daily about Internet related potential securities violations.

That centre, Walker said, has provided a number of leads on both new and current fraud investigations.

"Since the first Internet-related case we brought back in 1995, involving a scheme to sell unregistered securities in a worldwide telephone lottery over the Internet (SEC v. PleasureTime), to our most recent case involving a $7.2 million ponzi scheme peddled via the World Wide Web, we have done our best to keep the Internet safe for investors," Walker said.

"With the launching of this new unit, we hope to beef up our Internet presence and continue the success of our Internet Program."

Walker said John Reed Stark, the SEC's current special counsel for Internet projects in the Enforcement Division, will serve as chief of the new unit, the Office of Internet Enforcement, and Jay Perlman, a senior attorney in the Commission's Office of the Chief Counsel, will serve as deputy.

The 34 year-old Stark, with several years practising commercial litigation at Arent Fox Kintner Plotkin and Kahn, was named special counsel for Internet projects in 1995, after completing a seven-month detail as an Assistant United States Attorney for the District of Columbia, where he prosecuted criminal cases.

Perlman began his law career at the SEC in 1991, first in the Division of Corporation Finance where he was a staff attorney, then in the Enforcement Division's Office of Chief Counsel where he served as branch chief. Perlman also prosecuted criminal cases as an Assistant United States Attorney for the Eastern District of Virginia.

Walker said the new unit will operate at the SEC's headquarters in Washington, DC and will report to Joan McKown, chief counsel of the Enforcement Division.

Earlier this year, the SEC launched its Web service for investors to check on broker credentials.

The service, SEC Chairman Arthur Levitt said, gives individual investors "the power to be the first line of defence against fraud and abuse," and is available both online and by a toll-free phone number.

The service, he said, "presents, in a user-friendly way, the disciplinary and employment background for every registered broker and every registered firm in the United States."

Called the Central Registration Depository, the service is operated by the National Association of Securities Dealers, the groups that shares responsibility for regulating the securities industry.

The CRD, Levitt said, is part of a number of initiatives the SEC will launch, along with the enforcement unit, to close regulatory loopholes and strengthen the crackdown on fraud in the "microcap" sector of the economy, securities commonly called "penny stocks."

Levitt cautioned, however, that, while the CRD "helps you determine who you should not do business with, it doesn't give you the final answer on who you should do business with.

"Even after you've checked out a

broker's background and experience, you've got to make sure that you are comfortable with the style and approach used by the broker and his or her firm," he said. "That's why you still need to ask questions."

Hackers and Feds attack poor security

Hackers and federal agents faced off at the recent Black Hat Briefings in the US but they also found they had something in common: a lack of respect for the government's network security tactics.

"In general, we don't have a clue what the threat is and what ought to be done about it," said a Defence Department employee who identified himself only as Ken.

"Everybody basically does whatever he likes," said Marcus Ranum, a former hacker who characterised himself as a white hat.

"That's one of the reasons government security is so lame," Ranum said. "I'll believe the government is serious about security when somebody at the Pentagon gets fired."

The briefings brought hackers face to face with public- and private-sector systems administrators for two days of talks. Most panellists were identified by handles or first names only. The federal session barred photographers.

The hacker panel, despite casual attire, nevertheless represented corporate officials and consultants. Ranum, for instance, is president and chief executive officer of Network Flight Recorder Inc. of Woodbine, Md., a network monitoring tools maker.

One hacker, identified only as Artimage, said, "Right now I'm a college student, so I'm doing it for the grade. But next year, I'm in it for the money. I'm a whore; I admit it."

For the most part, the panellists presented themselves as ethical hackers who distinguished between breaking into systems and breaking code to identify weaknesses.

"The only people who really break into machines are malicious kids," said a hacker who called himself Peter.

The federal participants had even more complaints about government security practices than they did about hackers.

"A lot of managers have no idea where to start looking" for vulnerabilities, said a government auditor who identified herself as Ceil.

"I have become very cynical about the people who manage government systems and the vendors who are selling them things to secure those systems. You wouldn't sell a Porsche to a three-year-old who wanted a Matchbox car, but that's what they're doing-selling Porsches to dumb little three-year-olds," Ceil said.

She said parochial attitudes and stovepipe mentalities within agencies make it difficult to assess problems, let alone find solutions.

One federal employee, who performs vulnerability assessments for the Defence Information Systems Agency, defended government security efforts.

"We've got old management with old ways of thinking who need to be educated," he said, but "the government is not sitting idly by."

Flaws are getting identified and closed, he said. "It's a problem that is never-ending. Congress is throwing a lot of money at it."

Making a system Internet-accessible is asking for trouble, said a hacker identified as Mudge.

"There should be liability for not doing due diligence on your system when you've invited people in to take a look," he said.

Wisconsin online regulation

Wisconsin Lieutenant Governor Scott McCallum has announced his proposal to the state to adopt a range of Internet regulations he said were designed to "set some ground rules."

According to the Wisconsin State Journal, McCallum said basic rules need to be set up because "people are relying more and more on the Internet for personal and business purposes."

The package of reforms would allow Wisconsin Internet service providers to ban unsolicited junk mail, otherwise known as spam.

In addition, McCallum said he supports an Internet tax moratorium. Wisconsin is one of only eight states that currently charges a sales tax on ISP fees.

McCallum also said, according to the Journal, that privacy guidelines outlined in his proposal would require Web sites based in Wisconsin to tell their visitors what kind of information they are collecting.

Elsewhere in the state Internet tax moratorium arena, Massachusetts Acting Governor Paul Cellucci declared a 16-month moratorium on collecting a five per cent tax from ISPs. Florida, Washington, California and New York also have similar measures in effect.

Cellucci's measure would make the moratorium retroactive to 1990, costing the state a total of $7 million.

Regarding national efforts to ease Internet taxes, several governors this year have announced their support of the Congress' Internet Tax Freedom Act (S. 442), which is expected to encounter further Senate debate this fall.

Libel on the Internet

The Internet is ripe territory for ever-increasing numbers of libel suits, according to a new survey of attorneys.

The survey was conducted by The Affiliates, a staffing service specialising in project attorneys and legal support personnel. The question asked was "In the next three years, how do you think the Internet will affect the rate of libel lawsuits filed?"

Out of a poll of 200 attorneys from several different law firms, 68 per cent said they expect to see increased Internet usage to raise the rate of libel actions. Eleven per cent said the increase would be significant, while 57 per cent said the rate would increase "somewhat."

Fourteen per cent said there would be no change, and none of the attorneys polled believed there would be a decrease.

"While the Internet has become a major communications channel for both business and personal use, it is still in its infancy with regard to formalised regulation," said Affiliates Executive Director Kathleen Call.

"More libel actions continue to be filed as the courts determine how existing legislation and First Amendment issues apply to the online world."

The online medium certainly has raised the issue of the increased propensity for writing and posting incorrect or libellous information, especially when equal access is given, and furthermore is relatively easy to attain.

The affiliates is located at http://www.affiliates.com.

Thai Police Seize 79,000 Pirate CDs

Thai police have seized more than 70,000 pirated CD-ROMs, video CDs and music CDs with a face value of more than 20 billion baht ($476.76 million) in the biggest haul so far this year.

Two men were arrested after the raids, according to the country's Economic Crime Division.

Economic Crime Deputy Commander Pol Col Ekkarat Meepreecha said police suspected that the two men were part of a ring supplying pirated CDs and CD-ROMs to major computer shopping malls, including the most popular - Pantip Plaza.

Ekkarat said the police suspected that the leader of the ring was a Singaporean man, who has yet to be caught. Surawong Pongpaiboon and Anirut Suksai were arrested and charged with violation of copyright law and selling illegal goods.

Ekkarat said the haul included 23,433 CD-ROMs containing Microsoft software, 2,090 Video CDs containing movies from Goldstar Pictures, 1,365 CD-ROMs of Sony Entertaiment's computer games, and some 52,000 other CD-ROMs and pornographic Video CDs.

Ekkarat said the two alleged agents were supplying the pirated CDs to retailers at various spots in Bangkok. He said most of the CDs were produced in Malaysia and exported to Singapore before being imported to Thailand by the ring.

The raids, conducted on warrants issued by Thailand's Intellectual Property and International Trade Court, also netted two computers fitted out with recordable CD-ROM drives, police said.

The pirated material included copies of Microsoft's newly-released Windows 98 and software from Adobe, Autodesk, Lotus, Novell and Symantec, police added. Ekkarat said some of the Microsoft software had a registered value of US$40,000.

The pirated music CDs included material produced by Grammy Entertainment and albums by artists like Thatha Young and Thongchai McIntyre.

Pirated computer CD-ROMs sell for between 150 and 300 baht ($3.58 and $7.15) and some people have copied music CDs onto a new computer format know as MP3, which allows CD-ROMs to contain over 100 songs compared with just 15 songs on a normal audio CD.

Pirated MP3 CDs with a quality equivalent to audio CDs are known to be selling like hot cakes.

Disney e-mail offer is another hoax

An e-mail offering an all-expenses-paid trip to Disney World has been unmasked as a hoax - the latest in a long line of "urban legends" and chain letters that circulate online.

The new message, purportedly from Walt Disney Jr., claims that if it reaches 13,000 people, the first 1,300 who forwarded it will receive $15,000 "or a free, all-expenses-paid trip to Disney World any time during the summer of 1999."

Disney is well aware of the message and has fielded numerous calls. "Your first tip-off is that Walt didn't have any sons," a Disney operator commented. "Walt had two daughters," Disney spokeswoman Rebecca Buxton adds.

The message - with attached comments from people who claim to have called Disney to check it out - goes on to thank users for taking part in "Bill Gates' Beta E-mail Tracking" program, in which Disney is supposedly assisting.

"It is in fact a hoax," confirms Microsoft's Adam Sohn. "This one particularly doesn't even pass the giggle test. Our recommendation is that people don't pass it along and it will go away."

The message is a variation on an older chain letter e-mail featuring a supposed offer by Bill Gates to give $1,000 to the first 1,000 people who forward the message. That message first appeared in November of 1997.

The newer Disney version appears to be about two weeks old, says Bill Orvis, a hoax and virus tracker at the U.S. Department of Energy's Computer Incident Advisory Capability based at Lawrence Livermore National Laboratory in California.

"People seem to have learned that the Bill Gates one was a hoax. You'd think that they'd catch on that this was another one," Orvis says.

More information on chain letters and e-mail hoaxes is available at the CIAC Web site at www.ciac.org/ciac/CIACChainLetters.html.

Teen hackers could face adult courts

Concerned about threats to national security and angry at the amount of time and money teenage computer hackers cost the US government, some federal lawmakers want new laws to prosecute them as adults.

"This is a serious crime and we need to seriously bring the hammer down on them," Rep. Curt Weldon, R-Pa., said during a House National Security Committee hearing.

But not everyone agrees that prosecuting cyberspace delinquents as adults is a good idea. Local prosecutors worry that if Congress passes a law elevating computer hacking to an adult crime, they'll have to add new staff and spend more time building cases against junior high school students. That, they say, will drive their budgets up.

"The bulk of the cases will fall on local prosecutors and most are not equipped to deal with this at this point," said James Pauley, a spokesman for the National District Attorneys Association.

Child advocates also worry that prosecuting teenage hackers as adults could create problems in society later on when they try to get jobs despite having a permanent criminal record.

"We do try kids as adults when there is a heinous crime committed," said Leonard Nuara, a former New Jersey prosecutor who now specialises in computer law. "I just don't think this rises to

that level."

Although he opposes new legislation aimed at bringing teenage hackers to adult courtrooms, Nuara says hacking is a serious problem that must be dealt with.

Michael Yamaguchi, the US Attorney for the Northern District of California, agrees. His office prosecuted two teens who broke into government computers in January and February - at the height of the military confrontation between the US and Iraq. Both teens pled guilty recently and sentencing will be held later this year.

In their cases, the teens not only broke into sensitive government computers - including Air Force and the Lawrence Livermore National Laboratory systems - but also erased files in an effort to conceal their tracks.

Yamaguchi said that compromised the integrity of the computer systems and could have disrupted military communications worldwide at a time when the United States was on the verge of going to war.

Cracking the case required an extensive, and expensive, investigation by the FBI with help from NASA and Defence Department criminal investigations units.

Nuara and Yamaguchi are among those who want parents and teachers to take the lead role in combating teenage hacking.

But congressional patience may not last long enough for parents and teachers to do that. Weldon's comments drew immediate support from Rep. Herbert Bateman, R-Va., who agreed it's time to get tough with cyberspace delinquents.

"These kids need to know that this is not some kind of game," he said.

Paging hacker arrests

US firm PageNet claims to have successfully thwarted hacking attempts by Kenneth San Nicolas of San Diego, and says it passed to the FBI information resulting in his arrest.

PageNet says that the 18-year-old fraudulently created unauthorised voice mailboxes and paging accounts on PageNet's system.

San Nicolas' alleged activities were discovered by PageNet's systems integrity operation during an investigation into accounts with abnormal calling patterns. PageNet staff then monitored his activity on their system over a nine-month period, and turned over the information they gathered to the FBI.

PageNet says San Nicolas' alleged activities did not affect any PageNet customers. San Nicolas' activities, they say, did, however, end up costing the company more than $1 million in telecommunications charges.

"PageNet's Systems Integrity Group routinely studies the calling patterns of our customers to track abnormal call counts and potentially fraudulent or harassing use," said William G Scott, the company's senior vice president.

Hacking paging systems is a relatively new hacker activity. While voicemail systems have been successfully attacked since the mid 1980s, the first recorded "pager hack" in the US was in February,1998.

That hack affected several hundred Orange and Vodafone cellular subscribers and knocked out a UK textile company's switchboard for several days.

GSM cellular subscribers in the UK were text messaged using their phone's SMS (short message system) paging/text message service, and told they had won a prize, a Peugeot 106 car, and were to call a Nottingham number (the number of the textile firm) to arrange delivery.

After some investigation, the SMS messages were traced back to Omnipoint in the US, where it was discovered that an unknown hacker had dialled into the Omnipoint message server used for paging and SMS message users, apparently routing the messages to the UK cellular networks.

The hacker in the February incident has not been caught. For more information on PageNet, contact the firm on +1 972 801-8180

FBI predator booklet

The FBI in the US has published a booklet aimed at keeping children away from the potential dangers on the Internet and helping them to avoid online predators.

The booklet, called "A Parent's Guide to the Internet," has information for parents about how to keep their children safe from dangerous sexual predators who may be miles away.

FBI Spokeswoman Angela Bell, who specialises in matters of Internet safety for children, said that parents have expressed concern about what their children do online, an ether-world of semi-reality in which children often have a much greater understanding and facility than their parents.

"We've found a lot of kids online, and a lot of parents have no idea what their kids are doing," Bell said.

She added that the FBI has set up a separate area for children that teaches them the importance of maintaining safety and guardedness on the Internet as much as on the street.

The site also includes tips on "what to do if you suspect your child is talking to a sexual predator, and how do you minimise the chances of victimisation."

It contains tips on how to find cached pornography files on computers that children may have saved, and, perhaps most important for technophobe parents, it also includes a series of frequently asked questions and an Internet glossary.

Bell said the threat to children online from sexual predators is as real as any physical public location. "We have a lot of traveller cases. We arrest people who are specifically travelling with the intent of meeting children for sex purposes," Bell said. "We can prevent some man from molesting them. It's just as important as if we can stop a child from being raped or murdered."

According to the Web site information, predators "gradually seduce their targets through... attention, affection, kindness and even gifts... and are often willing to devote considerable amounts of time, money and energy in this process."

The FBI also lists several signs of online risk, including lots of solitary online use, especially nocturnally; hidden pornography on the computer; phone calls from strangers and long distance calls to unrecognised numbers; mail, gifts and packages from strangers; children who try to conceal the monitor from parents' gazes; withdrawn children; and the use of someone else's online account.

The FBI Web site is located at http://www.fbi.gov.

Product news

Tracking system finds stolen computers

A government office in the US recouped the $6,000 investment it made in notebook PC theft prevention software after it successfully traced lost systems.

The General Services Administration office in Atlanta recovered three stolen notebook computers, breaking up a ring of PC thieves in the process.

The Federal Protective Service traced the stolen notebooks using CompuTrace software from Absolute Software Corp. of Vancouver, British Columbia.

GSA spokesman Gary Mote said that the three recovered Toshiba America Information Systems Inc. Tecra 500CDT notebooks are worth between $3,000 to $5,000 each.

"The software is paying for itself," Mote said. The agency's Public Buildings Service bought 150 copies of CompuTrace for less than $3,000 in June 1997 and pays around $3,000 more annually in service fees.

About two weeks after the heist, the software vendor called the FPS in Atlanta with the phone number from which one of the stolen notebooks had been dialling.

CompuTrace sets a notebook's modem to call a server over a toll-free 800 number at regular intervals. The server records the date, time, and caller identification information and phone number.

With the number in hand, FPS officers got a court order to get subscriber information from the telephone company and also enlisted help from the Secret Service, Mote said.

The service got a search order and within 48 hours arrested a man who had the Tecra as well as a stolen Compaq Computer Corp. notebook, Mote said.

And the man, a native of Senegal, West Africa, gave information to FPS and Secret Service agents of a second Senegalese national, who had another of GSA's Toshiba Tecras and eight other stolen notebooks in his possession.

Charges against both men, at least one of whom was in the country illegally, have been dropped and instead the case has been referred to the Immigration and Naturalisation Service.

The two men had been sharing shopping lists of desirable notebooks to steal, Mote said. While working as GSA contract employees, they had taken the notebooks from a secured area without leaving any evidence, he said.

FPS officers speculated that the first man was using his two stolen computers to access bank accounts and attempt to commit financial crimes over the Internet, Mote said.

Dead Cow's Back Orifice kicked

A number of antivirus software firms have announced they have beaten the curious Trojan Horse program called the Back Orifice, from a group calling itself the Cult of the Dead Cow.

The cult appears to be allowing users of its Web site to download a DIY hacker's package that uses the Back Orifice software to gain unauthorised access to a user's PC.

Trojan, which is difficult to spot in normal PC operations, allows hackers to gain unauthorised access to high level commands on a user's PC, usually across an Internet TCP/IP (Transmission Control Protocol/Internet Protocol) connection, whether semi-permanent or on dial-up using a modem.

While Back Orifice is very difficult to detect, it apparently leaves a number of traces from its operations.

Microsoft has responded with assurances that the Trojan can be avoided by "safe computing" practices. In a statement at http://www.microsoft.com/security/mktBackOrifice.htm, Microsoft declared BackOrifice unlikely to threaten "the vast majority of Windows 95 or Windows 98 users."

"Like any other program, `BackOrifice' must be installed before it can run," Microsoft said. "Clearly, users should prevent this installation by following good practices like not downloading unsigned executables, and by insulating themselves from direct connection to the Internet with Proxy Servers and/or firewalls wherever possible."

According to one company, Internet Security Systems (http://www.iss.net), which issued a warning about the Back Orifice Trojan, the software runs under Windows 95 and Windows 98 and allows hackers to gain complete unauthorised access to a PC remotely.

ISS says that its antivirus package, RealSecure, can be set up to detect Back Orifice, which normally uses the UDP 31337 port to listen out for "hacker calls." ISS notes that Back Orifice does not run under Windows NT.

According to Trend Micro (http://www.antivirus.com), the cult says that more than 14,000 people have downloaded Back Orifice from its Web site, meaning that there are potentially more than 14,000 users capable of distributing the Trojan horse program and hacking a user's PC.

Trend has updated HouseCall, its free scanning software, available from the firm's Web site, to detect Back Orifice. The firm is also offering a 30-day evaluation version of its InterScan VirusWall software via its Web site.

According to Data Fellows, meanwhile, there is no easy way for a computer user to know an attack with Back Orifice is taking place.

Even worse, the firm says, there is no easy way to stop the attack once Back Orifice has installed itself on the computer.

Data Fellows says that, in a typical attack, the intruder sends the Back Orifice Trojan horse to his victim as a program attached to e-mail.

When the e-mail recipient executes the program attachment, the Trojan horse opens connections from the computer to the Internet. This allows the intruder to control the computer. The Trojan horse is invisible and will restart itself automatically even if Windows is rebooted.

Back Orifice then, the firm says, allows a hacker to view and modify any files on the hacked computer.

According to Data Fellows, the program can create a log file of the computer user's actions. It can take screen shots of the computer screen and send them back to the hacker - and it can be used to send messages to the user of the computer. Or it can simply crash the computer.

"Back Orifice is a seriously advanced tool for wannabe hackers," said Mikko Hypponen, Data Fellows' manager of antivirus research, who added that the

program presents little that is new.

"The Trojan horse still must be executed before it does anything. Back Orifice doesn't have any way to infiltrate the user's machine automatically," he explained.

According to Hypponen, Data Fellows has updated F-Secure Anti-Virus, its antivirus software, to handle the Back Orifice Trojan horse.

"We have to remember that Back Orifice is not a virus, it's just a simple Trojan horse. It doesn't spread by itself, and it doesn't attempt to replicate itself to users' files. Its attack doesn't escalate," he said. A free evaluation copy of the package is available on the firm's Web site at http://www.datafellows.com

Videodisc copy protection

Three firms are teaming up to merge their anti-pirating technologies in a bid to stop unauthorised copying of next-generation digital videodiscs and transmissions.

Macrovision Corp, Royal Philips Electronics NV and Digimarc Corp say they will merge their watermarking and play control patents and capabilities into a single system.

Macrovision will present the result for licensing by vendors to the Copy Protection Technical Working Group, an ad hoc group of Hollywood studios, consumer electronics manufacturers and PC hardware and software companies.

Other firms expected to field entries include an alliance between IBM and NEC, another between Sony and Hitachi, a system designed by Pioneer, and possibly another by Hewlett-Packard.

The Macrovision alliance will draw upon a combined base of 15 patents to design a foundation for a "viable commercial system," the firms said in an announcement. Such a system must satisfy - or at least not enrage - a welter of different interests, including the consumer electronics, information technology and content-creation communities.

In a video stream, watermarks can be added invisibly to each frame for extra robustness or can be inserted on any other definable basis. A detector in the playback or re-recording device then scans a stream to meet real-time play and record control requirements. The approach will work on most digital video delivery platforms, the firms said.

More information on the three firms and their products can be found on the Web at http://www.macrovision.com, http://www.philips.com and http://www.digimarc.com

Investigator program for download

WinWhatWhere Corp. has released Investigator 1.0, a program that detects and logs all Windows usage.

Once stored on a server, network administrators and other authorised users can backtrack to find problems in areas of security and human resource management, or can just use the program to keep a very detailed back up system.

Richard Eaton, WinWhatWhere president, said: "The program is perfect for corporations, government, or law enforcement agencies that need to keep tabs on security.

"The program works on any Windows-based system, whether it's a standalone system or small office/home office or large network. It's very networkable. You just point to the server and the program takes care of the rest."

He added: "Our keystroke monitor is the only one of its type, that puts keystrokes into the context of what a user was doing. The program will tell you what program the user was in, the time started and time spent and names of files opened."

The program watches the active area in Windows, the area on the screen that receives instructions from the user. Reports are given in two formats: one formatted, the other a raw, unformatted record of every back space, delete, function key, page up, page down, or arrow key.

The program can be run in hidden mode or can show an animated icon on the task bar. It also uses defensive measures to keep from being corrupted.

The program can be used to investigate computer crimes such as unauthorised access to accounting, financial, confidential or other sensitive files, Windows application productivity analysis, site license verification and analysis, discovering actual application usage, and interface analysis.

Eaton said: "If you think someone is getting into your accounting records, you would want to know everything that is going on in a specific computer or on all networked systems. You can install the program and remove it later, after your problem is solved."

Investigator runs as a 32-bit multithreaded program under Windows 95, Windows 98, and Windows NT systems. Eaton said that, to operate the viewing or playback portion of the program requires a minimum of 12 Mb of hard disk space and 8Mb of RAM.

But the "investigator" part of the program, the part that does the actual data collection, only takes up 140 kilobytes of space.

The evaluation version of Investigator is neither crippleware nor timed out, but rather always shows the splash screen. The program can be bought immediately for $285 per seat, with a declining cost per unit on volume purchases.

Eaton says the demo version is not crippled or timed out, but rather cannot be run in hidden mode. Users can download or purchase the software directly from the firm's site on the Web at http://www.winwhatwhere.com

For more information contact Richard Eaton at WinWhatWhere Corp on +1 509-585-9293 or +1 888-239-5396

Security probe service

International Computer Security Association and Gartner Group have announced a co-branded Internet Security Exposure Analysis service to detail a client's Internet security risks.

Neither firm sells security hardware or software, a fact they emphasise when discussing their lack of underlying marketing agendas.

The firms say they count on that objectivity to attract corporate customers that want an independent report of current risks. The idea is to leverage Gartner Group's research and analysis skills with ICSA's information security "attack"

expertise.

Peter Tippett, president of ICSA, stated, "We've found that many companies have embraced the Internet without first fully understanding the true security risks to their businesses."

He said ICSA's Internet Security Exposure Analysis would provide a "snapshot" of what areas a would-be attacker could exploit.

"The information received from this analysis provides an objective third-party report from which the client can confidently make informed network decisions," added Tippett.

At a minimum price of $25,000, the service is not targeted for small firms. However, since the price covers up to 500 Internet protocol (IP) addresses, midsized and large firms may find the price palatable for assuring their network security.

"Larger companies will understand what the issues are," predicted Japak. "the $25,000 is relatively inexpensive if you compare what is at risk.

If a company gets hacked they can lose data, competitive information, have their sites vandalised and have to deal with irreparable PR problems.

When you start adding up $25,000 against the consequences, it's relatively insignificant."

ICSA has a Web site at http://www.icsainc.com while Gartner Group's site is at http://www.gartner.com.

Or contact Kelly Clark, Gartner Group, 203-316-6449, e-mail kelly.clark@gartner.com

IBM's new safeguard for top encryption

IBM has announced a new "non-malleable cryptosystem" aimed at preventing two highly sophisticated methods hackers might use to decode encrypted messages without knowing the decryption key.

Called the CramerShoup CryptoSystem, the technology is likely to be included in a future edition of Vault Registry, which is designed to protect messages encrypted through SSL (Secure Sockets Layer) encryption schemes from being intercepted and decoded by unintended recipients.

Ashok Chandra, director of computer science at IBM Research Almaden, said that the new method, which is based on an algorithm developed by two IBM researchers, would work with "SSL and its extensions."

The basic approach used in the new CramerShoup Cryptosystem can be extended, however, to any public key encryption method, Chandra said.

The first of these methods involves "transforming" an encrypted message into another encrypted message. The second method calls for "sending a whole bunch of encrypted stuff, so (the encryption server) will leak information as to which is junk, and which is not junk."

The new CramerShoup CryptoSystem adds a series of new mathematical calculations that prevent the encryption server from transmitting clues about the decryption key that might be understood by highly knowledgeable crackers, according to the IBM computer science director.

Catching suspect keyboard characters

A miniature electronic surveillance device has been launched that captures keystrokes on a PC to help monitor a suspect.

MicroSpy can be fitted in seconds and captures the first 1,000 key presses by a user before its internal memory fills up, more than enough to record important information such as a password.

Once the device, a small nodule that simply plugs into the computer, has been used it can upload all the information onto the manager or investigator's own PC running Windows 95.

Its makers hope that MicroSpy will be used by police, IT staff and private investigators. For more information visit the Web site at www.microspy.com or telephone +44 01908 607007.

First Java virus

Symantec Corp has said its AntiVirus Research Center (SARC) has found a computer virus named Strange Brew that infects Java applets and applications.

Symantec calls it the first truly cross-platform virus, since it can infect any of the dozens of computing platforms that support Java.

SARC's automated virus-finding engine, a World Wide Web "spider" known as Seeker, found the bug during one of its routine forays into cyberspace. Seeker has scoured the Internet since 1996, gathering suspect files for analysis by the SARC lab.

Symantec's latest set of Norton AntiVirus definition files will contain a fix for the bug, the firm said. Symantec stressed that the virus is interesting mostly because it is a new type, since it does not pose a threat to users.

Carey Nachenberg, chief researcher for SARC, said that there is currently only one of these bugs and it carries no "payload" - that is, no instructions to do anything other than replicate - and it is flawed as well.

"It has a bug that will cause it to sometimes fail and corrupt the host Java file it infects," Nachenberg said. "It is not capable of spreading from within a browser. It is very badly written."

Strange Brew does have limitations. It can spread to Java executables only when an infected Java application, not a Java applet, is launched.

Most Java-enabled Web browsers have security features that would prevent such a bug from spreading. The virus also cannot use many of the nastier tricks invented for earlier virus types . For example, it is not likely to become polymorphic - that is, able to change its "signature" by modifying its internal code from one execution to the next - because, Nachenberg says, Java disallows self-modifying code.

SARC emphasized the virus was not found "in the wild," meaning it has not spread widely over the Internet. In fact, it doesn't really do anything except attach itself to Java executables and replicate.

As Nachenberg put it, "It's really only a proof of concept. It's a virus that just sort of hobbles along."

More on the Java virus and on SARC is available on the Web at http://www.symantec.com/avcenter or contact Symantec on +1 310-449-4309, e-mail glhaldeman@symantec.com

Year 2000 crime bug

Criminals are using the Year 2000 computer bug to steal billions of dollars in fraudulent billing scams, according to a new study. The review covered major financial institutions, health insurers and police agencies.

The findings from a review conducted by investigators at InfoGlide Corp are still in the preliminary stages, said John Valentine, chief executive officer of the firm.

He said: "Right now we can't demonstrate a lot of the live data because it's in litigation, but a good deal of it will be demonstrable after the first of the year. We'll have live data put up on the Internet - it will show fraud profiles."

He added, "It's kind of like we're a computer virus scanner, only what we find are criminal profiles. Once we discover a pattern of fraud, we can tell all the computer companies about it and they can go look for the profile."

The key to nearly all of these scams is fraudulent billing. The criminals count on sliding through channels undetected while defrauded firms and government agencies are diverted by the need to become Y2K-compliant before January 1, 2000. That's when the Y2K bug - which involves misinterpretation of dates labelled "00" instead of "2000" — will hit the hardest.

Staged car accident fraud rings are among the most common offenders. The fraud artists use modified names, addresses, social security numbers and "scores of other bogus identifiers," says the firm, to escape detection by harried IT departments.

Such rings stole up to $100 million from one major property/casualty insurance company alone, says InfoGlide.

The case was fairly typical. The perpetrators were computer-literate professionals who recruited computer programmers to use what InfoGlide calls Year 2000 "technology paralysis" to shield them. The programmers took advantage of built-in limitations of the neural net technology and relational databases used by most insurance companies and Medicaid/Medicare providers.

The key to the scam is that the databases use exact-match searching to detect multiple billings and other fraudulent practices. That leaves nearly unlimited room for the "devil to hide in the details."

The fraud artists typically change various identifiers - from single letters in their names to single digits in their US Social Security numbers - to take out multiple policies, stage multiple accidents, and continue collecting illegally.

Valentine says, "These computer criminals figured out the obvious. If they changed their names and addresses they could take out multiple policies. And they knew that the Y2K problems had the insurers too tied up to ever catch it."

In one fraud review, the firm listed 11 different, innocent ways to spell Los Angeles. Workers had simply made internal, non-fraudulent mistakes.

Criminals have found out about these limitations, Valentine says. In one unnamed US metro area, a ring of crooked doctors and lawyers hired immigrants to stage car accidents and investigators couldn't tell from one case to the next if they were dealing variations on the same unfamiliar names.

Remarked Valentine, "It's one thing when you have a policy for John James and Jimmie Jon, who an investigator might consider as the same person. It's much different with Nyuguen Hui Lao and Li Nyugen. The latter two are the same person, but you would never know."

InfoGlide says it based its review on interviews with attorneys, police organisations, private and government investigators, and prosecutors in 21 states. It also conducted interviews with insurance firms in Canada, the UK, and Australia.

According to Valentine, all have been hit by criminal fraud "as never before" at least partly because of Y2K paralysis.

Now the trend is mutating into more sophisticated scenarios. Con artists are changing every identifier, sometimes 30 at a time. They run scams across insurance, finance, and Medicaid databases, counting on the Y2K problem and what InfoGlide calls "its stranglehold on technical resources" to shield them from being caught.

Valentine said: "Y2K problems are freezing all the technical resources for the insurance and Medicaid industry. Y2K makes fraud a criminal's dream."

InfoGlide is on the World Wide Web at http://www.infoglide.com or e-mail jayinfoglide.com

• UK legal firm Tarlo Lyons has announced a Year 2000 moratorium that aims to reduce litigation due to the Millennium Bug.

Tarlo Lyons is the law company behind the six-pronged Pledge 2000 scheme unveiled by Action 2000, the UK government-backed Year 2000 agency. John Mawhood, a partner at Tarlo Lyons, is the author of the moratorium and the Pledge 2000 scheme.

Legal documentation for the moratorium is available on the Web for any organisation to use and apply. The Web address is http://www.tarlo-lyons.com/moratorium

According to Tarlo Lyons, the moratorium is similar in aim to President Clinton's plan for "Good Samaritan" legislation, which will work to clear the legal barriers that may prevent companies spreading good advice about Year 2000 readiness and fixes.

The law firm notes that, in the US, a value of $1 trillion has been estimated by Giga Information Group for Year 2000 related litigation.

The law firm says that the moratorium offers a framework for businesses needing legal protection to cover sharing Year 2000 information, and enable suppliers of IT systems and their customers to agree a temporary ban on legal actions, while also "stopping the clock" for time limits which could otherwise expire before the Year 2000.

Gwynneth Flower, Action 2000's managing director, said that the agency is supporting the moratorium.

"Any initiative that helps business direct all its efforts towards getting ready for the Millennium Bug is a welcome development," she said, adding that the agency is urging companies to continue the success of Pledge 2000 "and keep the channels of communication open."

Action 2000's Web site is at http://www.bug2000.co.uk and Tarlo Lyons' Web site is at http://www.tarlo-lyons.com or contact John Mawhood at Tarlo Lyons +44 (0)171-405-2000

Focus: On the Net patrol

Real-life law and order has come to the electronic frontier, even in the world's smaller communities. Police across the world are taking up an undercover tool: the Internet sting.

These frontier law officers generally are not experts or techie "geeks". Many are old-fashioned detectives with well-thumbed copies of Internet for Dummies.

They're looking for sexual predators who use the anonymity of electronic chat rooms and e-mail to find victims or trade kiddie porn.

James McLaughlin, a veteran of the force in Keene, New Hampshire in the US (pop. 22,430), is one such cybercop. Before his wife brought home a second-hand computer last year, he said, he knew next to nothing about the Internet. Now he cyber surfs almost daily, checking for any illegal activity.

His day begins with necessary deception. Within seconds of logging on to an Internet chat forum and posing as a teenage boy, McLaughlin, 41, is hit on.

"Want to trade?" the man writes, hoping to swap pictures of naked children.

"I am brand new," McLaughlin responds. "Can u send a few?" The cop won't transmit child pornography; he lets others make the first move.

"If you have self pics," comes the response.

McLaughlin sends a porn-free picture, supposedly of himself. "U like guys my age?"

"Yes... ."

A picture of an aroused naked boy appears on McLaughlin's screen at the Keene police station. The caption said he is 12 years old.

It is followed by a second, equally graphic photo of another boy, this one posing suggestively while pulling a shirt over his head.

A third image appears, of a fully-clothed man in his 30s, supposedly of the sender. "It's probably really him," McLaughlin said. "They're that stupid."

Stupid or not, they know he's out there. McLaughlin has a global reputation for taking down paedophiles. While posing as a teenager during an Internet chat with a suspected paedophile in Norway, McLaughlin got an eyeful.

"Watch out for this guy. He's out to get guys like us," the man warned, sending a digitised image of the detective taken from an article about his Internet sleuthing.

Another man living in Norway learned that the hard way. He and a Keene boy exchanged e-mail for months, and the two arranged to meet for sex.

But when the man arrived in Keene, the attractive boy turned out to be a middle-age man with a badge and a gun and the suspect was charged with attempted felonious sexual assault. If convicted, he faces up to seven years in jail, then deportation.

McLaughlin joined the police force in 1981 and specialised in sex offenders. He began focusing on Internet crimes about 18 months ago, when a Keene couple claimed that a woman was using e-mail to seduce their teenage son.

That's also when McLaughlin became aware of an article published by the North American Man/Boy Love Association, an organisation based in New York that advocates sex between men and boys, that gave instructions for using the Internet to find young partners.

McLaughlin guessed children using computers were revealing too much about themselves in chat rooms, putting themselves at risk. He was right.

As an experiment, he joined a chat frequented by youngsters from Keene. Using public records, he identified 80 percent of them. Predators, McLaughlin said, could do the same.

That's when he started exploring the sexual nether regions of the Internet. He didn't like what he found. "I was pretending to be a 13-year-old girl," he said, "and I had a guy who wanted to send me an airline ticket to run away."

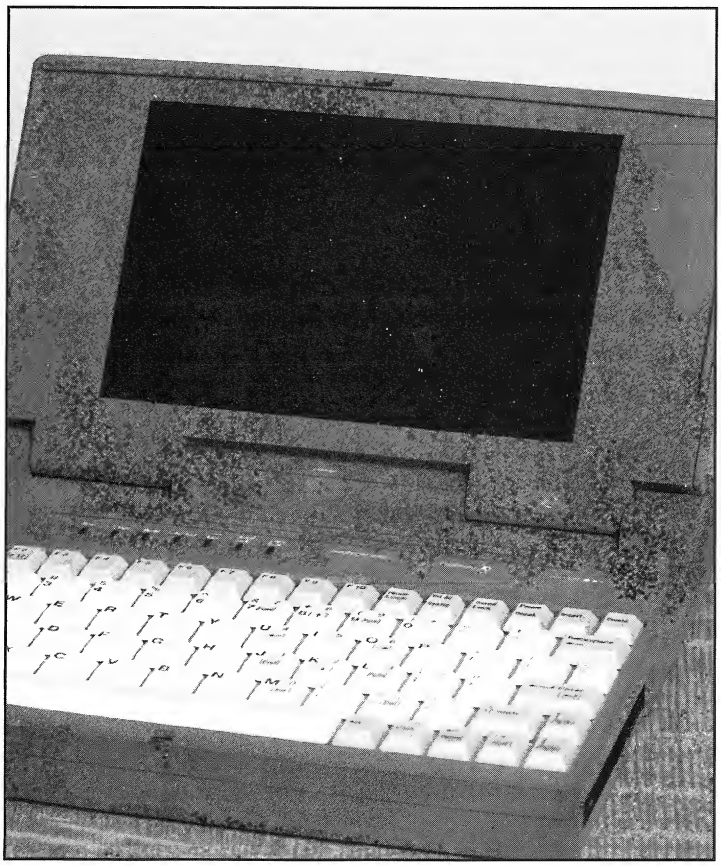
McLaughlin said he has to pose as a teenager to lure in those who might be looking for sex with youngsters. He uses the online anonymity that hides Internet stalkers to hunt the hunters.

"In less than a year I've busted more than 60 people," McLaughlin said. He has brought charges including travelling across state lines to have sex with children and distributing child pornography.

"If one officer in Keene, N.H., can do that, you can imagine how big the problem is."

Such success has prompted the FBI to take up the technique. This year, the agency hired 60 employees with expertise in computers and is spending $10 million to combat computer sex crimes.

One problem with fighting Internet sex crimes is the lack of a concerted na-



tional effort, McLaughlin said.

The task of enforcing child sex and pornography laws can fall on any number of federal, state and local agencies, including the FBI and US Customs. That also makes it difficult to determine the scope of the problem. Few national statistics have been compiled.

However, that could change as the FBI expands Innocent Images, a division charged with tracking the exploitation of children over the Internet. Since 1995, Innocent Images has made 161 arrests.

The group evolved from the hunt for a 10-year-old boy who disappeared in Maryland and was never found. The suspects routinely used computers to transmit child pornography and lure children to sexual encounters.

An accurate profile of Internet paedophiles remains elusive, McLaughlin said, as does research on differences between Internet and traditional tactics of exploitation.

Ten percent of McLaughlin's arrests involve suspects with prior convictions for molestation or child pornography. Fifty percent had ready access to children. Fewer than five per cent of child molesters are caught, he said - due mostly to a shortage of law-enforcement personnel. By the time molesters are caught, most have assaulted an average of 150 to 200 children.

And they aren't dirty old men, McLaughlin said. Many are married; most are techno-savvy. A significant number - 28 per cent - are still in college or high school.

McLaughlin's recent arrests range from Daniel Stage, of Germantown, Tenne., who sent him pictures of 12-year-old boys having sex, to Scott Hambrick, a police captain from Crozet, Va, who sent the cop's phoney boy-ego $270 to meet him.

Consequences can be severe. Stage, at 15 a minor himself, is charged with aggravated sexual exploitation of a minor. If tried and convicted as an adult, he could face twice that many years in jail and fines to $25,000.

The captain, 38, faces charges of sexually exploiting and coercing a minor over the Internet, with a penalty of up to 50 years in jail. Both are free, pending trial.

Though finding Internet paedophiles may not be hard, it is controversial. Some call it entrapment to pose as a child to set up phoney encounters. McLaughlin calls it fair play.

"We don't want to lull people into doing something they wouldn't normally do," he said. "We're not finding people on the flower channel or the baking channel. Affording someone the opportunity to do something criminal is not entrapment."

Not everyone applauds the crusade. Civil liberties watchdogs question whether police patrolling Web sites go too far.

"Innocent people are being brought into activity they would not otherwise engage in but for the guile and imagination of the police," said New Hampshire lawyer Mark Sisti, who represents three men arrested by McLaughlin.

"We're paying tax dollars to have police officers and FBI agents masquerade as nubile teenage girls," said Stanton McCandlish of the Electronic Frontier Foundation, a group that advocates Internet privacy.

Investigators say their critics are, at best, naive. They point to chilling case files:

- After one conviction for molesting a child in his hometown of Framingham, Mass., janitor Michael Austin was watched closely; he could no longer go near a school or playground without attracting police attention.

He began using a computer bulletin board to contact young boys by advertising items for sale. Two who met him to buy items were raped. Austin is in prison.

- When Sharon Lopatha of Maryland disappeared in 1996, police checked her home computer for clues. They learned she had posted messages in a forum devoted to sexual sadism. Her body was found in North Carolina, buried in the front yard of a man who browsed the same forum.

- On July 12, police in Holden, Mass., arrested a convicted sex offender from Michigan. They say he drove there to meet a 16-year-old girl with whom he had corresponded in an Internet chat room. The girl was running toward his pickup with a suitcase, police said, when they stopped her.

"This isn't a crime that's going to go away. As more and more people go online, the problem will grow," said Doug Rehman, a former state of Florida investigator who now teaches others how to combat computer vice.

But some police officers say patrolling the Internet is not always an efficient use of time. Others say police should focus instead on school programs promoting Internet safety.

"There are Web sites dedicated to hacking, cult recruitment and dangerous pranks," said Al Olsen, police chief in Warwick Township, Pa. "I tell parents, 'Don't think you can drop off your kids on the information highway without any worries.'"

Others worry that Internet illiterates could fall prey to overzealous cybercops if they accidentally surf onto a child pornography Web site.

McLaughlin calls that unlikely. The people he's after have at least 1,000 pornographic images on their computers, he said, and some have 40,000, with elaborate databases to organise them.

Part of the problem is the sheer number of children using computers, and they often are more computer-literate than their parents are. So, McLaughlin said, being aware of technology and of how children are using the Internet is the best way for parents to ensure safe surfing.

In Keene, McLaughlin has helped federal agents bust a New York man who met with more than 20 teens he had contacted online.

McLaughlin describes the more than 60 suspects he has helped bring in as men aged 13 to 60 from all walks of life.

"Almost half of them have kids of their own or jobs involving kids," he said. "We've arrested a dozen schoolteachers, six ministers and priests, police officers and a psychologist."

For now, McLaughlin sits at his computer, facing an image of an adult man having sex with a young girl. He shakes his head. Some days it's tough to come to work.

"We're not talking about a New Hampshire problem, or a national problem," he said. "It's a global problem. That becomes overwhelming at times."

Global paedophile ring

Police and law enforcement officers across the globe swooped on suspected child pornographers in one of the biggest busts of its kind.

The homes of more than 100 people in 14 countries were raided in the operation, dealing a massive blow to a ring of online paedophiles. Paul Johnson reports.

In probably the most important anti-child porn action so far, more than 40 people were arrested around the world for their suspected part in an illegal operation peddling paedophile material across the Internet.

The UK National Crime Squad co-ordinated the raids as part of a five-month investigation into the so-called Wonderland club, which authorities said exchanged pornographic pictures of children as young as two on the Net.

During the investigation, code-named "Cathedral," police said they found a database containing more than 100,000 pornographic photographs of naked boys and girls and confiscated computers and computer programs from dozens of suspects. The largest amount seized prior to that, officers said, was 10,000 pictures.

Police said they targetted 180 suspects and arrested 48 in the raids, which took place on three continents - in countries including Australia, Austria, Belgium, Britain, Finland, France, Germany, Italy, Norway, Portugal, Sweden and the United States.

"I am unaware of another police operation that has ever pulled together so many law enforcement agencies worldwide to effect simultaneous raids and arrests," said Bob Packham, deputy director general of the National Crime Squad in the UK.

He said: "It has been a difficult and distressing investigation and I hope that our actions have prevented further abuse of children across the world."

The Wonderland used sophisticated codes and passwords to protect its electronic library of tens of thousands of images from discovery.

"There is a possibility that as we go through the operation, there may be more people that feature in what we recover," said Jackie Bennett of Britain's National Crime Squad.

"This particular group is very significant. What they were dealing with, these images, were horrific," Bennett said. "But we don't know if other similar clubs exist."

British police said the majority of those arrested were men but some were women and some of the children whose images were used in the paedophile club were related to those arrested.

In the UK, police arrested 11 men in a raid on 14 addresses and in the US Customs officers issued 32 federal search and seizure warrants in 22 states with four arrests.

The National Crime Squad said 10 people were arrested in Germany, eight in Norway, five in France and three in Italy. Police in Sweden also reported one arrest, and four arrests were reported in Australia.

German investigators said they have now detained five more additional suspects as part of the operation and still more could be rounded up.

The Federal Criminal Agency (BKA) said a total of 23 people had been detained in Germany since the co-ordinated operation began. Most were released after questioning.

Suspects from Berlin, Stuttgart and Naumburg had confessed to exchanging child pornography and information over the Internet, German police said.

The BKA said it did not have a precise picture of how many computer terminals and video cassettes had been seized. In some cases thousands of files had been taken, a spokesman said.

Britain's Detective Superintendent John Stewardson, who led the global operation, said children had been abused on a massive scale to produce material to feed the international ring.

"The content would turn the stomach of any right-minded person. It's really disgusting," he said.

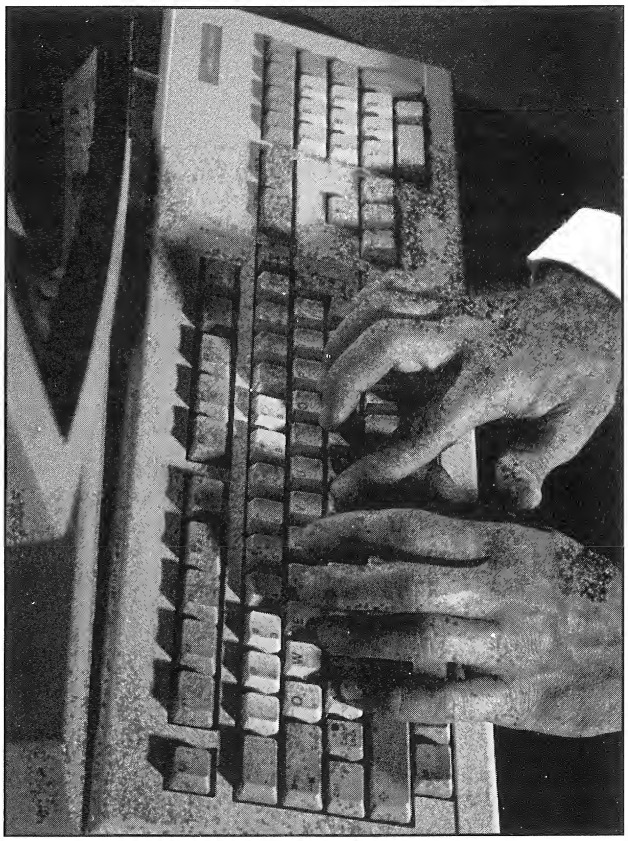
He added: "There are people who simply exchanged material and some who produced it. We have got one producer in the UK who was part of this group.

"The children abused were of both sexes and some it would appear were as young as two, although we don't know because we don't know who these children are yet."

He said the club had left a "horrendous legacy" through the number of children abused to feed it material.

DS Stewardson said: "I am confident this operation has targeted the hard core of individuals engaged upon Internet paedophile activity around the world."

He said child pornographers had felt relatively secure up to now in the knowledge that the Internet was virtually



unpoliced.

"They have been able to continue their practices with impunity. This co-ordinated action around the world today has demonstrated that this is no longer the case," Stewardson added.

Police said they would now attempt to trace some of the children in the pictures and pledged that efforts would now be made to trace all the children involved across the world to give them the help they needed and to assist bringing their abusers to justice.

Although the Wonderland club was set up in the United States, its activities only came to light during an investigation by Sussex Police in the UK.

Interpol headquarters in France said British authorities had sought their assistance "when it became clear the arrests of the ring members, in almost constant contact over the Internet, would have to be very precisely co-ordinated."

Police officials from the participating states had met over the summer at Interpol headquarters to prepare the action.

"Crime on the Internet is a global phenomenon which requires a global approach," Ralph Mutschke, Interpool assistant director for criminal intelligence and liaison, said in a statement.

Ease of Net porn

The Internet has become fertile ground for paedophiles looking for material to feed their depraved urges, as the "Wonderland" club shows.

Detectives said the club used sophisticated techniques to cover its electronic tracks and to keep access to material secure.

Using anonymous e-mail addresses, routing messages through re-mailing services which strip them of any identifying features, and encrypting material before sending it all make it difficult to pin down the sources of the millions of pieces of information sent via the Internet.

This difficulty is aggravated by the international nature of the forum.

Crossing national boundaries, paedophile material read in the UK can originate overseas and messages between ring members can be sent via foreign service providers.

Investigations are reliant on police forces co-operating, often within very different legal systems, as well as technical know-how. It is, police admit, an obvious forum for paedophiles.

However the officers at the heart of this worldwide operation are hoping it sends out a clear message that the Internet is no longer as anonymous and faceless as paedophiles might like to believe.

A combination of greater technological awareness among law enforcers, better co-operation between police forces around the world and the willingness of the industry to help, has made it easier to track people who send illicit material across the networks.

David Kerr, of the Internet Watch Foundation, set up to monitor child pornography on the Net, said: "The Internet is a lot less anonymous than people often think.

"It's far better documented than anything like the post or telephone calls and it's relatively easy to track people down and today's operation shows that police are getting increasingly good at doing that."

However, the amount of pornography on the Net is still growing.

In its first year of operation, the Internet Watch Foundation received around 2,300 reports of illegal websites.

This year Mr Kerr expects that figure to be closer to 5,000. Mr Kerr said: "We see the tip of the iceberg, and don't know what's underneath."

Commenting in a statement on the crackdown, US Internet business trade group the Internet Alliance said it supports the action.

"The Internet Alliance has long held that this abhorrent material has no place in society and that our organization has an absolute responsibility to be part of the solution in its removal," the group said.

"Today the US Customs Service sent a very strong signal that existing laws can and must be enforced," said Internet Alliance Executive Director Jeff Richards.

"The Internet Alliance and its members co-operate fully with law enforcement. Those who seek to exploit children and the Internet see today that there is no place to hide."

The UN Educational, Scientific and Cultural Organisation (UNESCO) said it was convening a conference of experts in January to discuss paedophile activity on the Internet.

"This is the recruiting ground, and then people go into more closed communication," said Nigel Williams, director of Childnet International, a British-based body promoting the interests of children in Internet communications worldwide.

"It is now so easy for people to contact each other for good or bad purposes, which presents a series of dangers," Williams said.

"The issue is these are pictures of real children. Who is that child? When did it happen? Is it happening now?," he added.

Electronic mail passed over the Internet also makes it faster and simpler for photographs, in electronic form, to be sent around the world with relative anonymity, said Edward Wilding, a consultant with Network Security in London.

"It is very difficult to monitor this sort of activity," he said. "If you send information between two sites in a secure way, it is impossible to track information."

Frustration at the apparent easy availability of child pornography has inspired some computer hackers to turn vigilante, either bombarding those trading child porn with junk e-mail and computer viruses or infiltrating the system and wiping off websites containing illicit material.

The crackdown is inspired by the realisation that, behind the images of children on the screen, lie real youngsters who have been subjected to appalling sexual abuse.

Although some paedophiles create images which look like children by doctoring pictures of adults, most of the images are not computer-generated.

As police who sifted through the Wonderland Club's massive database said, every electronic picture is evidence of a "horrendous legacy" of child abuse to feed an international desire for child pornography.

On the trail of criminals - how the UK police investigated

Some 20 officers were assigned by the National Crime Squad in the UK to investigate the ring in April and had been working since then in conjunction with police forces abroad and computer experts to track down members of the club.

Officers who led the operation said 11 men had been arrested in the UK following raids on 14 addresses in London, Sussex, Oxford, Berkshire, Kent, Gloucestershire, Middlesex and Norfolk and West Lothian.

Some of the images were generated in the UK, with one of the men arrested in the UK described as an active "producer" member of the group.

The international investigation was sparked by Sussex police who stumbled across evidence of the Wonderland Club while probing a separate organisation, known as the Orchid Club after a tip-off from US customs.

Officers in the US investigating the so-called Orchid Club handed a name and address in Hastings to English detectives who then raided the property earlier this year.

A man in his late 20s was arrested and a computer seized, but only when material stored on it was examined did it become apparent that he was heavily involved in an unconnected paedophile network now known to be the "Wonderland" club.

He was released on bail as investigations continued and has now been re-arrested following the world-wide raids.

Detective Chief Inspector Dave Wood, head of Sussex Police's Intelligence Bureau, said: "We went and had a look and found the computer and discovered this completely unconnected club. He was just a conduit, not a leading light. It's not a Sussex based international network, he was just a member.

"We then did as much as we possibly could with regard to the information stored on the computer and realised it had worldwide implications and handed it over to the National Crime Squad.

"It was through the work of Sussex officers in connection with a separate investigation that the existence of this huge international network was uncovered."

US Customs vow to go after child molesters

"People try to smuggle in smut just like they try to smuggle dope across the border and we're ready to pounce on them," said Dick Weart, a special agent for the US Customs Service, which carried out 32 raids in 22 states with the help of state and local police.

There were four arrests, but only when there was material evidence, such as a print-out, or one of the subjects of a photograph, in plain view.

Police confiscated "boxes of pornography, various software materials and hardware that were part and parcel" of the ring during the raids, Weart said.

To join the child pornography ring, members had to have multiple images of child pornography, and some had as many as 10,000 pictures, US Customs said. The ring allegedly began in the US.

"The people who exploit children in this way think they can hide in cyberspace. They are wrong. We will find them and bring them to justice," US Customs Commissioner Raymond Kelly said.

Weart said the investigation's next step would be to identify the children pictured.

"This investigation is about bringing these criminals to justice and hopefully saving some children from an awful existence that they certainly don't deserve," Weart said.

While this investigation began in Britain, it grew out of a large Customs investigation on the West Coast that culminated in 1996, Weart said. "A lot of the information gleaned from that investigation was given to our British counterparts" and the other countries, he said.

The states where raids occurred were California, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Kansas, Maine, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, New Jersey, New York, North Carolina, Oklahoma, Pennsylvania, Texas, Utah and Virginia.

The authorities now are examining the hard drives of seized computers to determine if and/or where child pornography is cached.

The Customs Service said it opened the first federal law enforcement programme into computer child pornography in 1989, and the first similar case in the online medium in 1993.

In 1997, the agency arrested 173 people on child pornography charges, and secured 158 indictments and 178 convictions. In the fiscal year 1998 (Oct. 1,1997, to present), the agency has arrested 183 individuals and made 189 convictions. It also has made 181 indictments.

• A German citizen living in the US suspected of involvement in the international child pornography ring was found dead in his home after his wrists were slashed, probably by himself.

The man is thought to be a 35-year-old microbiologist working at a laboratory at the University of Connecticut Health Centre in Farmington. He was found in his bathtub and had allegedly cut his wrists. According to reports, the Connecticut Medical Examiner ruled the death a suicide.

Australia tackles porn

Australian Police involved in the worldwide swoop on Internet child pornography said Australia was the second biggest downloader of child pornography in the world.

Western Australia state's police child abuse unit, which arrested a Perth man, said Australia was second only to Germany for downloading child pornography. Detective Mick Miller said police seized computers and several CD-ROM's with pornographic images of children.

Australian Justice Minister Amanda Vanstone said the success of Operation Cathedral sent a clear message to Internet child pornographic rings that the world's police were prepared to co-operate internationally to end such child abuse.

"We've been able to be very successful against an alleged Internet paedophile club," she said. "It sends a very clear message to people who want to exploit the Net that Australia has federal and state police forces that are ready, willing and capable of pursuing this sort of crime."

Investigation techniques

Hierarchical Structured Investigation (HSI™)

By Peter Verreck

The problem of the information volume

A major problem facing the forensic analyst is volume of information. The average size of a hard disk today is 2.6Gb and this may contain an enormous number of files.

Between 10,000 - 15,000 files are quite normal. Some hard drives have in excess of 30,000. This is an easy number to say but anyone who has had to look through that amount of information is aware of just how huge and time consuming the task can be.

Not only is there a logistical problem in sorting through the information, but also it is easy to get 'lost' and to lose sight of the objective of the investigation.

To avoid some of the pitfalls, and to give a reference point from which to work, we use a structured method of investigation called Hierarchical Structured Investigation or HSI™.

HSI™ requires the investigator to work in an organised manner and to move from one level of the investigation to another based on information about the type of crime suspected and the background of the suspect. Additionally it provides the investigator with guidelines to suggest when an analysis should stop.

In order to use HSI™ the analyst must first understand the concept of levels of investigation.

Levels of investigation

Computer forensic analysis can proceed at different levels according to the nature of the case, the information sought and found and details concerning the background of the suspect.

By levels we mean the type of space occupied by the information on a hard disk. Generally speaking the examination becomes more time consuming the deeper the level of analysis.

The first level of analysis is the active files. These are the easiest to access and view and they should be eliminated from the investigation before moving to a deeper level. The next level is deleted files. These are relatively easy to access but they can be time consuming to undelete.

At a deeper level still is slack space and deeper still are unallocated space and orphaned clusters. Finally a full structural analysis can be carried out using advanced cluster analysis and statistical techniques.

This can reveal information such as sequences of events on a computer hard disk. However it is very time consuming and demands a high level of technical ability.

If one performed a full analysis on each and every drive it would take a very long time to complete an investigation. Therefore one needs to have a means of deciding how far to go and when to stop.

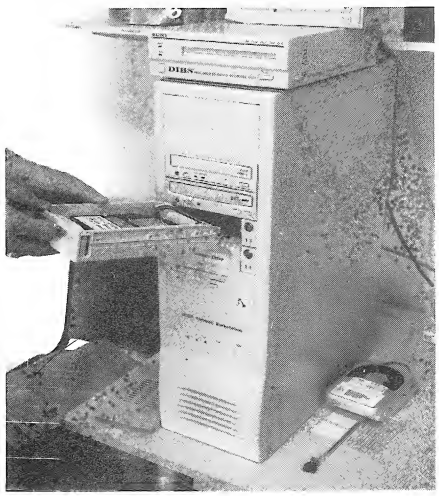
The most important principle used here is that if sufficient information has been obtained at one level of analysis there is no need to move to a deeper level. Stop at this point. If necessary the analyst can always go back again at a later date.

The investigator can move from one level of analysis to another depending on the information found at the higher level.

For example if the analyst is seeking to find evidence of possession of child pornography and has found thousands of active graphics files containing this type of material there is no need to look any further. There is sufficient evidence to present to the court for this offence.

The investigator can stop the analysis stage and move on to presenting the evidence.

If, however, he or she is also looking



Level of forensic analysis

Depth of analysis	Levels
↓	Active files
	Deleted files
	Slack space
	Unallocated space
	Orphaned clusters
	Structural relationship

for proof of distribution and has found nothing in active files then they may need to look deeper at the deleted files, and possibly beyond, to find the evidence.

Knowing how far to go and when to stop requires you to keep a clear view of the objective of your investigation in terms of the type of crime suspected and the background of the suspect. This must be regarded from a computer viewpoint.

Maintaining focus

At the commencement of an analysis and at regular times throughout, it is important to take time to carefully consider where you are going.

Never be afraid to stop and think about what you are doing.

Or better still discuss it with someone else. As in all types of investigation it is much better to work as a team of two than on your own.

Think at all times about exactly what it is you need to find in order to pursue your case.

As you proceed with your analysis you will find paths leading off in unexpected directions.

Be careful if you start to follow these. They may be very interesting but they will not necessarily advance your investigation and may occupy a great deal of your most valuable and finite resource - time.

A good example of falling into this trap involved a case of charity fraud where the key document was a forged employment contract. This was proving difficult to recover amongst a vast amount of information.

One sub-directory contained numerous documents concerning property transactions. The analyst spent a great deal of time examining these in detail and they proved to be most interesting.

However, they were of no value to the case being pursued and although they might form the basis of further enquiries, to date they have been of no use.

The suspect was convicted with the originally sought evidence. The case is now two years old and it is unlikely that the unnecessary work will ever be used.

The golden rule is stop and think about what you are doing and stay focused.

Case background - type of crime

In considering the approach you will take to your investigation carefully consider the type of crime you are examining in relation to the computer. Think about the type of information you will require.

It may seem obvious to say that you should know about the type of crime but it is surprising how often someone will commence an investigation without any real idea of what they are looking for.

Sometimes this is because they have been handed a computer by a third party and simply asked to 'find the evidence'. Other times it is because they have not thought about what they are doing.

For example, if you have a case involving forged documents, then think about how they would be produced. If it is a false agreement you are looking for then this will most likely be produced by a word processor. What word processor is on the document? What extension does it assign to files?

If it is Word for Windows then the most likely extension is DOC. Look for active files with extension first before looking elsewhere. This will be quick and easy to do. If you find what you are looking for then there is no need to go deeper.

Similarly if you are looking to prove possession of pornography you will want graphic files. The most common extensions for these are JPG, BMP and GIF. It is simple to produce a file listing and then sort the files by extension to locate these.

If, however, you are seeking to prove distribution of pornography then the type of information sought will probably be within a communications program.

It will be log files showing that transmission of material has taken place. Or it may be in e-mail messages. These will then be linked to the actual files which should exist on the hard disk.

In each case it is only by careful consideration of the nature of the computer investigation that a starting point can be found and the analysis begin.

Case background - profile of suspect

Having established the type of information sought the next problem is to know how deep to go in the analysis.

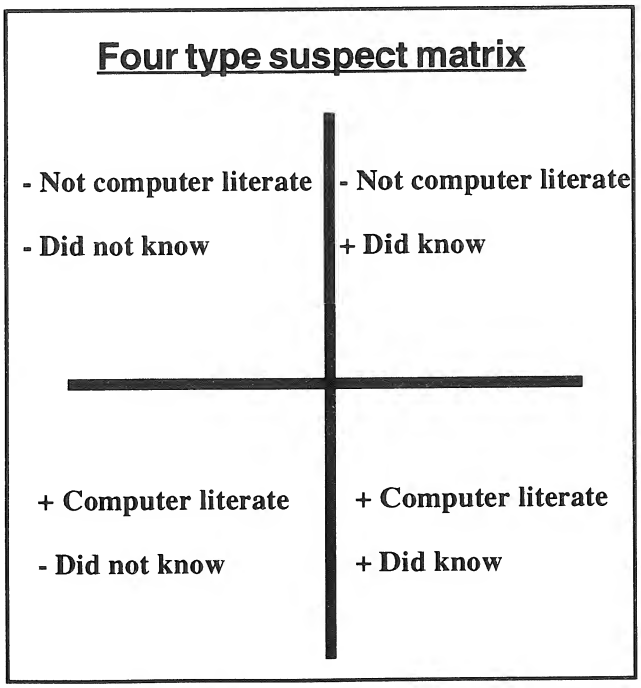
The general rule is to stop once you have found sufficient evidence to support your case. However, what if you have not found the evidence - is it the wrong computer? Is it on another unseized machine? Is it the wrong suspect? You do not want to spend a large amount of time on a 'wild goose chase'.

To give some guideline about how far to go we use information about the suspect. The two pieces of essential information we need, and which you should obtain about each suspect are:

· Is the suspect computer literate?

· Did the suspect know about the investigation prior to the raid?

Consider this information in terms of the four main possibilities as shown in the matrix below.



Lets look at each of these cases individually.

Not computer literate - did not know about the investigation

This person uses a computer but has little or no understanding of how a computer works. They had no idea they were under suspicion and did not expect to be raided and have their equipment seized and examined.

The most likely place to find information is in the active files and possibly in deleted files. It is unlikely that anything will be hidden since they do not possess the skill to do this and they had no reason to do so.

In this case if there is nothing in active and deleted files it is less likely that it will be found elsewhere. Look for other computers, or media such as floppy disks, and consider other suspects. This is the circumstance in the vast majority of cases.

Not computer literate - did know about the investigation

This person does not understand how the computer works and has no knowledge of the way in which the information is stored and arranged.

However, they found out that they were under investigation prior to the raid. In these circumstances the most likely place to find evidence will be in the deleted files.

The action they are most likely to have taken before the computer was seized was to have deleted incriminating files in the mistaken belief that this would remove the evidence. In reality they have just pointed you to the exact location of the evidence.

This type of circumstance is quite common. For example, in one investigation the suspect was about to board a plane in the USA to return to the UK when a call was received from an accomplice.

This told the suspect that there was an investigation under way. On boarding the flight the suspect spent the first two hours, until his battery ran out, carefully deleting every incriminating file from the hard disk of his laptop.

On arrival in the UK he was arrested as he left the plane and his laptop was seized. A quick and simple analysis revealed all the evidence in the deleted files, which were undeleted, printed and presented to the suspect on the same day as his arrest. Faced with this evidence he made a full confession and pleaded guilty to the charges.

Computer literate - did know about the investigation

This tends to be a fairly straightforward case, although not very common. The most likely scenario is that the information is not on the computer. Or if it is, it is well hidden.

This is a case where you need to very carefully consider just how deep you go in your analysis. You could easily spend a great deal of time looking for something that is not there.

Consider the individual. He knows all about computers. He knows he is being investigated. He is unlikely to have left anything incriminating in any obvious place.

He is quite likely to have 'cleaned' his machine. Or to have a second unknown, hidden machine. However, do bear in mind that if his offence involves the use of computer based material he is unlikely to have just thrown it away. It is most likely stored somewhere. Check other media and in particular floppy disks.

This was the circumstance in the Black Baron virus writer case. Here a highly computer literate person knew he was under investigation. He therefore 'cleaned' his machine in such a way that no trace of his criminal activities remained on the hard disk.

A 'cleaned' machine is easy to spot for the experienced forensic analyst and on seizure and examination this was immediately apparent. The analyst therefore spent no further time on this item but turned his attention to the floppy disks also seized.

He knew that the suspect would have spent a great deal of time and effort in creating the virus and he reasoned that he would not have completely destroyed his 'creation'. Using a statistical technique to analyse the type of files contained on the floppy disks he quickly isolated a suspicious file contained on a mouse drivers disk.

It was named as if it was a program file but on further examination it was found to contain the source code to the virus stored in a compressed form. The evidence was presented to the suspect within hours of the seizure. He confessed and pleaded guilty.

Computer literate - did not know about the investigation

This is the most difficult circumstance. The suspect knows all about computers but did not know about the investigation.

It is reasonable to assume that if nothing is found in the higher levels it could be elsewhere, hidden in areas or files not immediately apparent. This is the case where a full analysis may be unavoidable but fortunately it is comparatively rare.

Of course between these main categories there are grey areas where only partial information about the suspect is available, or none of the categories fit perfectly. But in these circumstances it is found in practice that careful consideration of the factors involved enables a considered judgement to be made to maximise the efficiency of the investigation.

Evaluating evidence

At all stages of the analysis stop at regular times and evaluate the information you have obtained. Is it suitable for use as evidence? Does it support your case? Is it sufficient? Does it really mean what you think?

Discuss the case with others and show them the information you have obtained. Tell them how you interpret it and what your conclusions are. We are capable of drawing the wrong conclusion from a piece of information and it is better to be corrected by a colleague than, at a later date, by a barrister in a court of law.

Knowing when to stop

Having performed your analysis, obtained and evaluated your evidence know when to stop work. If you have sufficient

evidence to pursue the prosecution do not keep on analysing just for the sake of it.

You will be wasting your valuable time. It might be interesting and satisfying to find more information but if it does not help your case then your time would be better spent doing something else.

If you have found nothing, think about the four circumstances in the matrix above before delving deeper and deeper. Is it the right computer? Is it the right suspect? Are you looking for the right type of information?

Most experienced analysts have made the mistake at least once of spending a great deal of time looking for something that does not exist. Stop and think carefully before you go too deep. Learn when to stop.

Extending the concept

The concept of HSI™ is useful not only for the examination of individual items but also for a batch of items. If you are faced with a number of computers in an investigation try to find out which is the most likely to contain the information. Copy and examine this one first.

If you find sufficient evidence there may be no need to go further and examines the other machines. Similarly, if you have floppy disks do not examine these if you have already found sufficient evidence on the associated hard disk.

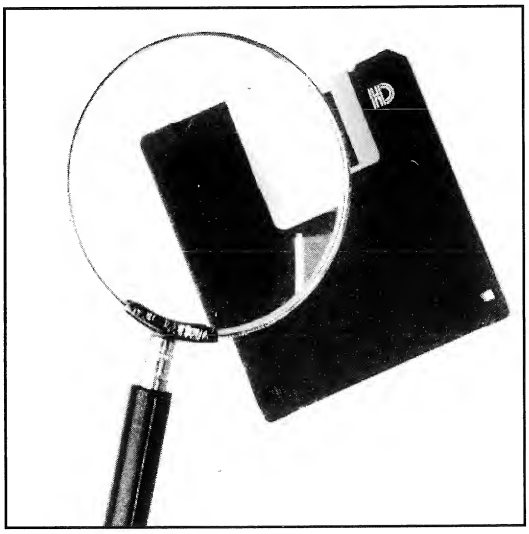
If you have a batch of floppy disks start the examination with those that were nearest the machine and therefore are most likely to have been used. Leave until last the dust covered 5.25" floppy disks found in the attic and only examine them if nothing has been found elsewhere.

An example of this method in action was seen in a recent case where sixteen computers were seized. Enquiries revealed that three of the computers were the most likely to contain the required information.

They were copied and analysed and produced sufficient evidence for the prosecution to proceed. The other thirteen computers were retained but not examined.

Peter Verreck is managing director of Computer Forensics Ltd in the UK.

Q I have seized some Iomega Zip disks which I am informed are protected by a password. How can I gain access to information on these disks?



A There are two ways to handle this situation. Both methods rely on the low level of security that the Iomega Zip drives employ. When a zip disk is protected all that happens is that a 'flag' is set that tells the computer that this disk requires a password and its contents should not be displayed without one.

The data on a Zip drive is not encrypted. In each case the security built into the driver (the software provided to allow the operating system to operate the Zip Drive) is by-passed.

The first method, and forensically the safest, is to image the Zip disks using a SCSI Zip drive in the normal way, thus by-passing 'flag' check. The data contained on the images can then be processed in the normal way.

The second method should only be used when it is absolutely necessary to access the actual Zip disk itself. One instance where we had to employ this method was when ordered, by the court, to wipe a number of password protected Zip Disks containing child pornography and return them to their owner.

1) Install a Zip drive and its associated drivers in your workstation.

2) Using the Iomega utilities set the Drive to powerdown after one minute of inactivity.

3) Then insert a clean Iomega Zip Drive, protect this disk with a password (make a note of it).

4) Access the drive and activate the 'unprotect until Eject' option of the Iomega Utilities. To ensure the disk remains unchanged also enable the write protect option.

5) Wait one minute for the drive to 'sleep'.

6) Insert a straightened paper clip into the small hole on the back to eject the disk without the drive waking.

7) Insert your suspect's Zip Disk.

You now have access to the data on the disk.

This must be done with extreme caution - experiment with this method before using it on a 'live' case. Remember that write-protecting a Zip disk or unprotecting by the usual means will change data on the disk.

Q I have seen that Windows 98 Plus pack has a feature called 'compressed folders', what is this and how can I deal with it forensically?

A The compressed folders option is simply a different way of viewing standard zip compressed archives. Using compressed folders a zip file appears as a folder and its contents are accessed by entering that folder.

When examining a disk that has compressed folders on it using an operating system other than Windows98/ Plus 98 they are listed as standard zip files.

With that in mind the techniques you currently use for examiningz zip files should work for compressed folders.

Thanks to Chris Crute, Kent Police, for this month's Q&A.

E-mail questions, comments or suggestions, to the Journal at ijfc@pavilion.co.uk

Notice Board

We will be pleased to receive contributions to this page. Please mark all correspondence 'Notice Board'. We reserve the right to edit if required.

Events

Security in Large-Scale Distributed Systems in conjunction with Symposium on Reliable Distributed Systems

20-23 October 1998 Purdue University, W. Lafayette, US

Contact: Prof. Eugene Spafford
e-mail: spaf@cs.purdue.edu

Documents Group Meeting

26 November 1998 The Royal Society, London

This meeting will see new developments in tools and techniques in forensic document work and will be addressing controversial areas of modern forensic science such as the qualification of forensic scientists and the scientific basis of handwriting comparison.

Programme includes "Looking to the Future, Qualifications and the Institute of Forensic Science", papers exploring the scientific basis of handwriting comparisons.

Technical session includes Raman Spectroscopy work, and other papers dealing with wall writing, counterfeit documents, fax document distortion and shredded documents.

Contact: Anne Holdsworth, FSS Tel: +44(0)1423 506068 Fax: +44(0)1423 566391

Emerging Trends in Financial Crime

2-3 November 1998 London

This conference will bring together representatives from financial institutions, regulators, law enforcement agencies and private sector security organisations to examine the likely future trends and developments in financial crime around the world, and to discuss what can and should be done to counter the growing threat facing the world's financial system.

Contact: Int. Conference Group Ltd Tel: +44(0)171 499 0888 Fax: +44(0)171 499 5722

Internet Gaming Industry conference

Nov 29 - Dec 1 at the J.W. Marriott in Washington, D.C.

The conference is sponsored by Gaming Law Review and the atmosphere will be distinctly Caribbean, featuring speakers such as Antigua Prime Minister Lester Bird and Dominican representative Aretha Francis. Since online gambling centres currently are illegal in the United States, offshore-based betting has become popular for the online audience.

Sessions will include forecasts for the world markets in online gaming, international mechanisms for industry regulation, e-cash systems, financial management IPOs and Wall Street issues, security issues, successful Web site operation, regulatory compliance and enforcement, money laundering, online sportsbook activity, the potential for Internet lotteries, Native American Internet gaming and airline-based online gaming.

Contact Pat Hogan for BioConferences International Inc on +1 914-834-3100 ext. 611

Securecomm 98

November 8-12, 1998, Capital Hilton, Washington, DC.

During Securecomm 98, there will be more than 50 presentations on topics such as: E-commerce, PKI, IP Telephony, Protecting Intellectual Property, Telecom Security and Legal/Regulatory Issues.

To register, access the home page at www.bellcore.com/securecomm or call Maureen Dunne at Bellcore at +1 (732) 758-5370.

Next month

In the October issue of the Journal we feature an in-depth look at cryptology and key encryption and we also examine the discussions in the UK to give police greater access to private e-mail.

Published by
Computer Forensic Services Ltd.